Mutually unbiased bases, Latin squares and orthogonal pairs(Group Theory and Related Topics)

AUTHOR(S):

綿谷, 安男

CITATION:

綿谷, 安男. Mutually unbiased bases, Latin squares and orthogonal pairs(Group Theory and Related Topics). 数理解析研究所講究録 2007, 1564: 138-149

ISSUE DATE:

2007-07

URL:

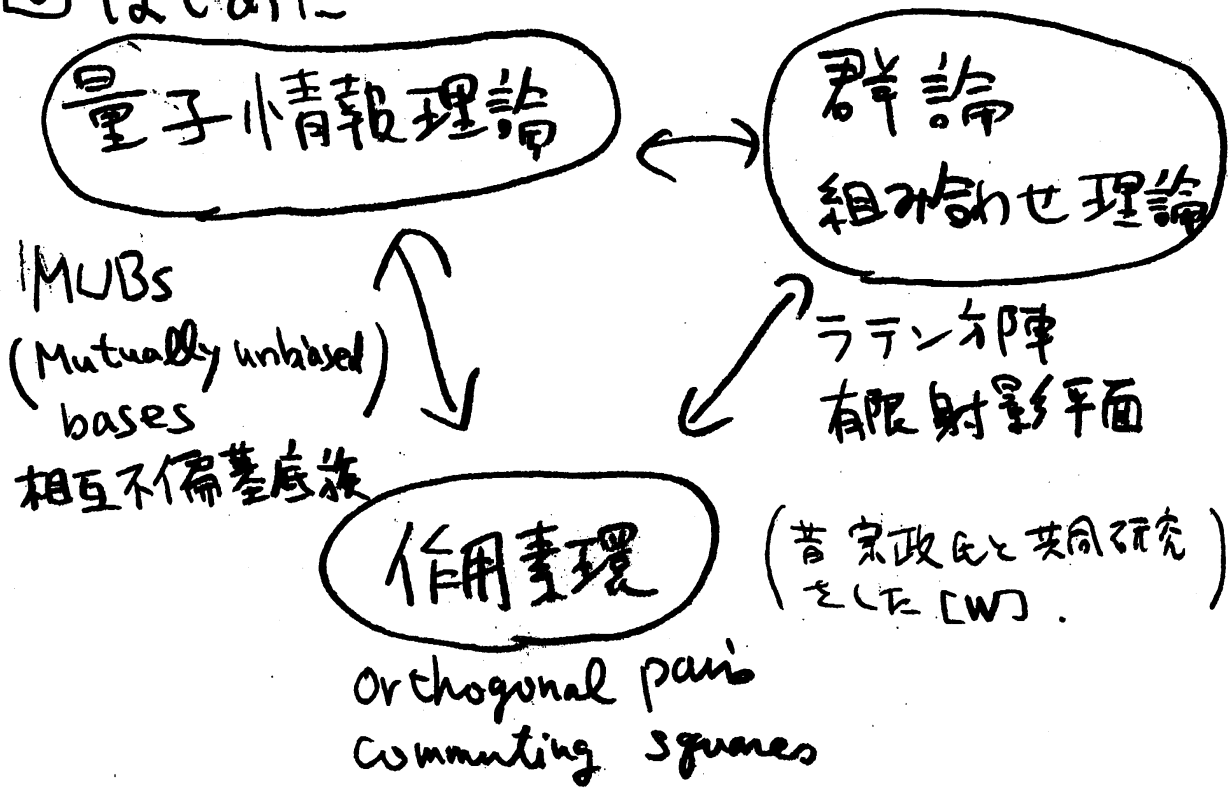
http://hdl.handle.net/2433/81134

数理解析研究所講究録
1564 巻 2007 年 138-149

Mutually unbiased bases, Latin squares and Orthogonal pairs

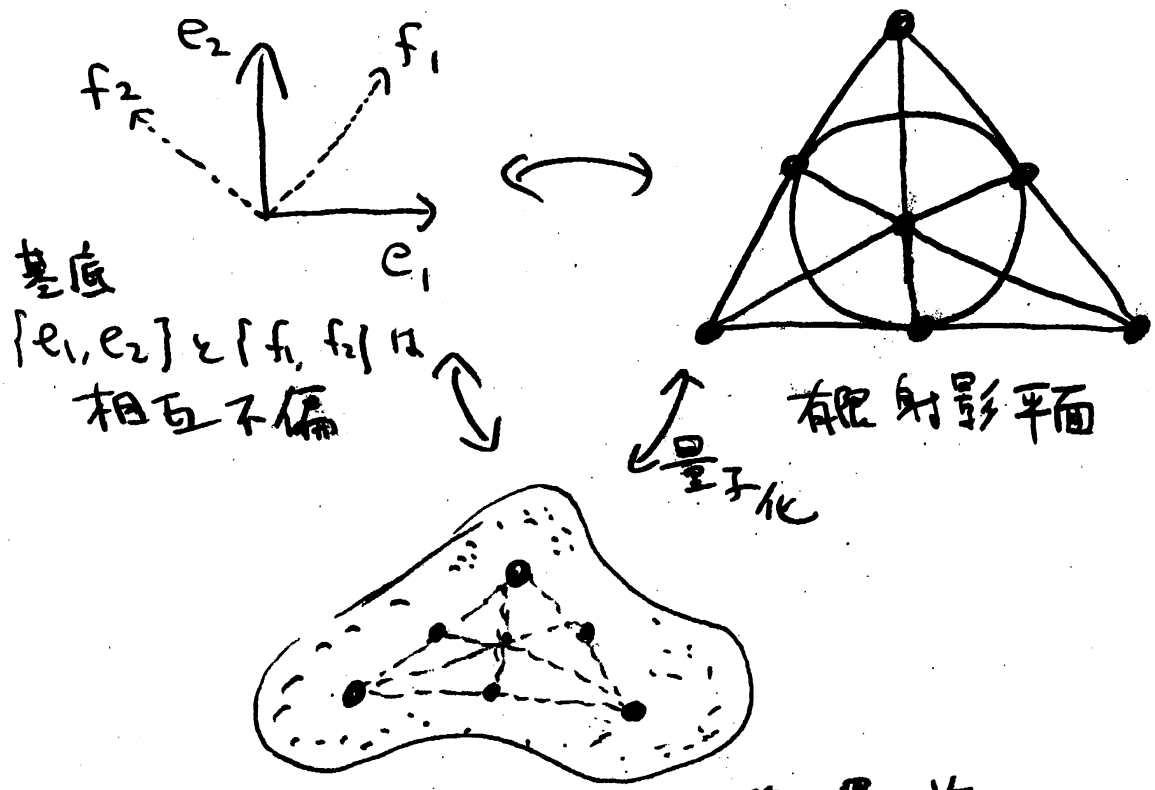
九州大学・大学院数理学研究院 綿谷安男
Kyushu University Watatani, Yasuo

0 はじめに



このノートでは，上の図式にあるように，3つの異なる分野，量子情報理論，作用素環，群論・組み合わせ理論に関係があることを紹介する．

象徴的な対象を絵にしてみよう



行列環の3つの極大可換環の族

① 有限次元ヒルベルト空間の2つの基底が「相互不偏」である。

② 2つのラテン方陣が「直交」する

③ 行列環 $M_n(\mathbb{C})$ の2つの極大可換環が $\mathbb{C}I$ を除いて直交する (orthogonal pair である)。

(はみんなよく似た概念で作用素環の commuting square の概念で統一できる。

1 MUBs (Mutually Unbiased bases)
相互不偏基底族

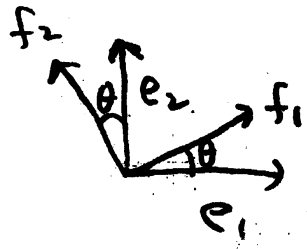
例 $H=\mathbb{C}^2$ を2次元のヒルベルト空間とする

$\mathcal{E}=\{e_1, e_2\}$ を標準基底とせよ。

つまり $e_1=\begin{pmatrix}1\\0\end{pmatrix}$, $e_2=\begin{pmatrix}0\\1\end{pmatrix}$ とする

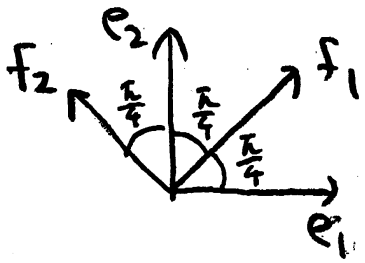
$\mathcal{F}=\{f_1, f_2\}$ を他の基底をとる。

$\mathcal{E}$ と $\mathcal{F}$ が「互いに偏よっていない」をうまく定義したい。



f_1 は e_1 には近いが e_2 には遠いのでこれではダメ。

そこで θ を $\frac{\pi}{4}$ に変えてみる：$f_1=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$, $f_2=\frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix}$



$|(e_1|f_1)|=\frac{1}{\sqrt{2}}$, $|(e_1|f_2)|=\frac{1}{\sqrt{2}}$

$|(e_2|f_1)|=\frac{1}{\sqrt{2}}$, $|(e_2|f_2)|=\frac{1}{\sqrt{2}}$

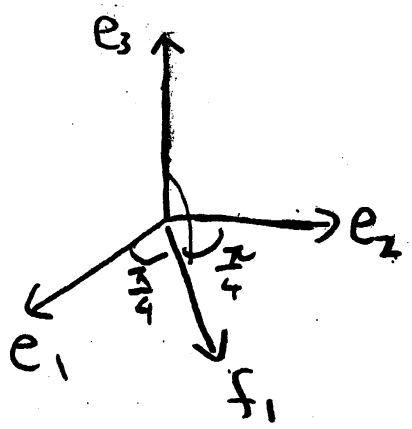
そこで $\mathcal{E}$ と $\mathcal{F}$ が相互不偏とは $|(e_i|f_j)|=\frac{1}{\sqrt{2}}$ とする。

例 $H=\mathbb{C}^3$

$\mathcal{E}=\{e_1, e_2, e_3\}$ を標準基底とせよ。

つまり $e_1=\begin{pmatrix}1\\0\\0\end{pmatrix}$, $e_2=\begin{pmatrix}0\\1\\0\end{pmatrix}$, $e_3=\begin{pmatrix}0\\0\\1\end{pmatrix}$ とする

$\mathcal{F}=\{f_1, f_2, f_3\}$ を他の基底とする。



$f_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\end{pmatrix}$ とおいてみると

f_1はe_1とe_2とは同じ位離れているが，f_1とe_3はそれらよりずっと離れている。

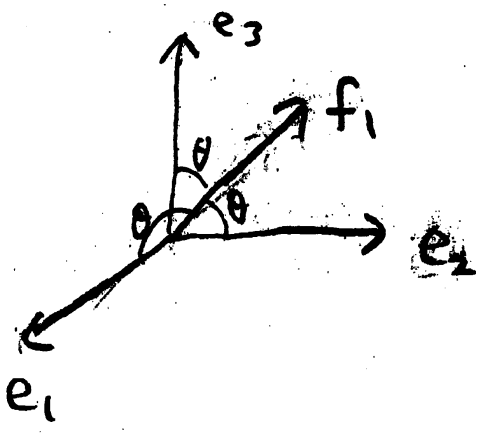
$(e_1|f_1) = \frac{1}{\sqrt{2}}$，$(e_2|f_1) = \frac{1}{\sqrt{2}}$

$(e_3|f_1) = 0$　直交している

f_1がe_1, e_2, e_3の3つと偏りなく離れているようにするにはどうとればよいか？

$f_1 = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\1\end{pmatrix}$

がよさそうだ。



$|(e_1|f_1)| = \frac{1}{\sqrt{3}}$
$|(e_2|f_1)| = \frac{1}{\sqrt{3}}$
$|(e_3|f_1)| = \frac{1}{\sqrt{3}}$
← 偏りなく離れている

残りのf_2とf_3もe_1, e_2, e_3の3つと偏りなく離れているようにしたい。ωを1の原始3乗根の1つとして

$f_2 = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega\\\omega^2\end{pmatrix}$，$f_3 = \frac{1}{\sqrt{3}}\begin{pmatrix}1\\\omega^2\\\omega\end{pmatrix}$ とすると $|(e_i|f_j)| = \frac{1}{\sqrt{3}}$

$i, j = 1, 2, 3$ とできる。これで相互に偏りなく離れた。

Def $H=\mathbb{C}^n$：n次元ヒルベルト空間

$\mathcal{E}=\{e_1, e_2, \cdots, e_n\}$ ：a basis

$\mathcal{F}=\{f_1, f_2, \cdots, f_n\}$ ：a basis

$\mathcal{E}$と$\mathcal{F}$が mutually unbiased（相互不偏）

$\overset{\text{def}}{\Longleftrightarrow} \forall i, \forall j \quad |(e_i|f_j)| = \frac{1}{\sqrt{n}}$

Def $H=\mathbb{C}^n$ のMUBs（Mutually Unbiased bases）

（相互不偏基底族）の中で極大なものの個数

を $N_{MUB}(n)$ とかこう

例 $N_{MUB}(2)=3$

$H=\mathbb{C}^2$ で次の3つの基底 $\mathcal{E}, \mathcal{F}, \mathcal{G}$ をとればよい

$\mathcal{E}=\{e_1, e_2\}$, $\mathcal{F}=\{f_1, f_2\}$, $\mathcal{G}=\{g_1, g_2\}$

$e_1=\begin{pmatrix}1\\0\end{pmatrix}$, $e_2=\begin{pmatrix}0\\1\end{pmatrix}$, $f_1=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$, $f_2=\frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix}$, $g_1=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$, $g_2=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$

例 $q=p^k$：素数pの中 $\Rightarrow N_{MUB}(q)=q+1$

$H=\mathbb{C}^q$ で ω を1の原始q乗根とする

$a, b \in \mathbb{F}_q$ に対し、$v_{a,b} := \frac{1}{\sqrt{q}}\left(\omega^{\mathrm{Tr}(ax^2+bx)}\right)_{x\in\mathbb{F}_q} \in \mathbb{C}^q$

$\mathcal{E}_a := \{v_{a,b} \in H \mid b\in\mathbb{F}_q\}$ は basis

$\Rightarrow \{\mathcal{E}_a \mid a\in\mathbb{F}_q\} \cup \{\text{標準基底}\}$ がMUBsで q+1コ

問題 $N_{MUB}(n) = n+1 \Rightarrow n$は素数冪か？

は未解決の問題です。

$N_{MUB}(2) = 3$, $N_{MUB}(3) = 4$, $N_{MUB}(4) = 5$ですが
$N_{MUB}(6)$を求めることすら，まだ未解決です。
$N_{MUB}(6) \geq 3$しかわかっていない。

2 組み合わせ・群論

極大相互不偏基底族の数$N_{MUB}(n)$と大変類似したことは組み合わせ論でよく知られています。

問題 nを素数冪とした時，位数nの有限射影平面が存在します。その逆である。
位数nの有限射影平面が存在 $\Rightarrow n$は素数冪か？
は未解決の問題です

又た位数nの有限射影平面の存在
$\Leftarrow$ 位数nのラテン方陣で互いに直交するものの
極大なものの個数$N_{MOLS}(n) = n-1$
はよく知られている。

≪相互不偏な基底と直交するラテン方陣は類似がある≫

Def $A=(a_{ij})_{ij}$ が位数 n の ラテン方陣

$\overset{\text{def}}{\Longleftrightarrow}$ A は 各成分 a_{ij} が $\{1,2,\cdots,n\}$ からなる $n\times n$ 行列で どの行 とどの列にも $\{1,2,\cdots,n\}$ が 2回以上 現れない.

Def 2つのラテン方陣 $A=(a_{ij})_{ij}$ と $B=(b_{ij})_{ij}$ が 直交する

$\Longleftarrow$ $\{(a_{ij},b_{ij})\mid i=1,\cdots,n,\ j=1,\cdots n\}$ は すべて 異なる対になっている.

例 $A=\begin{pmatrix}1&2&3\\2&3&1\\3&1&2\end{pmatrix}$, $B=\begin{pmatrix}1&2&3\\3&1&2\\2&3&1\end{pmatrix}$ は 位数3の ラテン方陣で

$$(a_{ij},b_{ij})_{ij}=\begin{pmatrix}(1,1),&(2,2),&(3,3)\\(2,3),&(3,1),&(1,2)\\(3,2),&(1,3),&(2,1)\end{pmatrix}$$

とすべて異なる対が 現れるので A と B は直交する

Def 位数 n のラテン方陣の中で 互いに直交する 族の中で 極大な ものの個数を $N_{MOLS}(n)$ とおこう。

例 $N_{MOLS}(2)=1$, $N_{MOLS}(3)=2$, $N_{MOLS}(4)=3$

$N_{MOLS}(5)=4$, $N_{MOLS}(6)=1$, $N_{MOLS}(7)=6$

$N_{MOL}(8)=7$, $N_{MOLS}(9)=8$, $N_{MOLS}(N)\geq 2$

量子情報理論	組み合わせ理論
ヒルベルト空間の基底	ラテン方陣
次元	位数
相互不偏	直交
$N_{MUB}(n)$：相互不偏な基底の族で極大な個数	$N_{MOLS}(n)$：互いに直交するラテン方陣の族で極大な個数
$n \geq 2$ $\Rightarrow 3 \leq N_{MUB}(n) \leq n+1$	$n \geq 2$ $\Rightarrow 1 \leq N_{MOLS}(n) \leq n-1$
nが素数の巾 $\Rightarrow N_{MUB}(n) = n+1$ 逆は予想で未解決	nが素数の巾 $\Rightarrow N_{MOLS}(n) = n-1$ 逆は予想で未解決
nが素数の巾の時の例の構成は有限体を使う	nが素数の巾の時の例の構成は有限体を使う
$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \geq 2$ と素因数分解されている $\Rightarrow N_{MUB}(n)$ $\geq \min\{ p_i^{e_i} + 1 \mid i = 1, 2, \cdots, r \}$	$n = p_1^{e_1} p_2^{e_2} \cdots, p_r^{e_r} \geq 2$ と素因数分解されている $\Rightarrow N_{MOLS}(n)$ $\geq \min\{ p_i^{e_i} - 1 \mid i = 1, 2, \cdots, r \}$
小さいnでも決定は難	小さいnでも決定は難

相互不偏基底族については最近のreview [B] とそこにのっている文献をみてもよう。群論を使った構成とその限界については [ACW] がよい。$N_{MUB}(n)$ と $N_{MOLS}(n)$ との間の評価式については次が知られている。

Theorem (Wojcan-Beth) [WB]

$$N_{MUB}(k^2) \geq N_{MOLS}(k) + 2$$

3 作用素環による統一

相互不偏基底と直交ラテン方陣の話は類似があるというだけでなく作用素環論における Jones の部分因子環理論 [J] において使われた commuting square の概念を使うと統一的に扱える。

ヒルベルト空間 H 上の有界作用素全体 $B(H)$ は $*$ 環になるが，弱作用素位相で閉じた部分 $*$ 環を von Neumann 環，作用素ノルム位相で閉じた部分 $*$ 環を C^* 環という。以下では finite trace $\tau : M \to \mathbb{C}$ をもつ von Neumann 環 M を主に考える。M に内積を $(T|S) = \tau(S^*T)$ で入れて Null で割り完備化して $L^2(M,\tau)$ とおく。

Def A, B, C を M の *subalg とする

$$\begin{array}{ccc} A & \subset & M \\ \cup & & \cup \\ C & \subset & B \end{array}$$

が commuting square を成す

$\overset{\text{def}}{\Leftrightarrow}$ $\begin{cases} C = A \cap B \\ L^2(A) と L^2(B) は L^2(C) を除いて直交する \end{cases}$

つまり $\left(L^2(A) \ominus L^2(C)\right) \perp \left(L^2(B) \ominus L^2(C)\right)$

特に $C = \mathbb{C}1$ となるときは A と B は orthogonal pair を成す ともいう [P].

例 $M = M_n(\mathbb{C})$: $n \times n$ 行列全体

$H = \mathbb{C}^n$ の basis $\mathcal{E} = \{e_1, e_2, \cdots, e_n\}$ をとり

$\mathbb{C}e_i$ への Projection を P_i とおく; $P_i(x) = (x|e_i)e_i$.

$A(\mathcal{E}) := \{\sum_{i=1}^n \lambda_i P_i \mid \lambda_i \in \mathbb{C}\}$ は $M_n(\mathbb{C})$ の極大可換環になり, 逆に $M_n(\mathbb{C})$ のどんな極大可換環も H のある basis $\mathcal{E}$ をとって $A(\mathcal{E})$ という形をしている。例えば $\mathcal{E}$ が標準基底なら $A(\mathcal{E})$ は対角行列全体のなす環である。この意味で

$$\{\mathbb{C}^n の基底\} \overset{1:1}{\longleftrightarrow} \{M_n(\mathbb{C}) の極大可換環\}$$

Proposition $H=\mathbb{C}^n$ 上の basis $\mathcal{E}=\{e_1,\cdots,e_n\}$ と $\mathcal{F}=\{f_1,\cdots,f_n\}$ をとってくる。$M_n(\mathbb{C})$ 上には正規化された trace $tr: M_n(\mathbb{C})\to\mathbb{C}$ が存在する
この時次は同値：
① 基底 $\mathcal{E}$ と $\mathcal{F}$ は相互不偏
② 極大可換環 $A(\mathcal{E})$ と $A(\mathcal{F})$ は orthogonal pair in $(M_n(\mathbb{C}),\cdot)$ ← 通常の積

例 $A=(a_{ij})_{ij}$ を n 次のラテン方陣とする。これをアダマール積 $\circ$ とみた $(M_n(\mathbb{C}),\circ)$ の元とみる。

$$P_k(i,j)=\begin{cases}1 & (a_{ij}=k)\\ 0 & (a_{ij}\neq k)\end{cases}\quad \text{とおくと}$$

P_k は $(M_n(\mathbb{C}),\circ)$ の projection になり，

$A=1P_1+2P_2+3P_3+\cdots+nP_n$ はスペクトル分解

そこで $\mathcal{B}(A)=\{\sum_{k=1}^n \lambda_k P_k \mid \lambda_k\in\mathbb{C}\}$ とおくと $\mathcal{B}(A)$ は $(M_n(\mathbb{C}),\circ)$ の可換部分環。

Proposition 上で $(M_n(\mathbb{C}),\circ)$ 上には $\tau(A)=\frac{1}{n^2}\sum_{i,j=1}^n a_{ij}$ で trace をあたえる。A と B をラテン方陣とすると次は同値
① ラテン方陣 A と B は直交
② 可換環 $\mathcal{B}(A)$ と $\mathcal{B}(B)$ は orthogonal pair である

(注) つまり $M_n(\mathbb{C})$ 上の通常の積・とアダマール積 $\circ$ の違いだ。

≪References≫

[ACW] M. Aschbacher, A. Childs, P. Wocjan, The limitation of nice mutually unbiased bases, to appear J Algebr. Comb.

[J]. V. Jones, Index for subfactors, Invent. Math. 66 (1983), 1-25.

[B]. I. Bengtsson, Three ways to look at mutually unbiased bases, arXiv: quant-ph/0610216, (2006)

[P]. S. Popa, Orthogonal pairs of "subalgebras in finite von Neumann algebras, J. Operatn. Theory, 9 (1983), 253-268

[W] Y. watatani, Latin squares, commuting squares and intermediate subfactors, "Subfactors" (1994) 85-104,

[WB] P. Wocjan and T. Beth, New construction of mutually unbiased bases in square dimensions Quantum. Inform. Comput. 5 (2005), 93-101.